Fighting untrustworthy Internet content

Prins, J.E.J.; Schellekens, M.H.M.

Published in:
Information Polity

Publication date:
2005

Information Polity 10 (2005) 129–139
IOS Press

Fighting untrustworthy Internet content: In search of regulatory scenarios[1]

J.E.J. Prins and M.H.M. Schellekens
Tilburg Institute for Law, Technology and Society (*TILT*), *Tilburg, The Netherlands*
E-mail: {j.e.j.prins, m.h.m.schellekens}@uvt.nl

Abstract. The question of liability for the consequences of misleading information on the Internet is deeply problematic. The information chain can be long and pass through several jurisdictions *en route* from information supplier to information consumer. Organisations along the chain, such as ISPs, which attempt to provide quality or reliability checks, are inhibited from so doing by potential liabilites if they make public statements about their filtering policy. Self regulation would seem to offer one possible solution, but here too there are difficulties in both enforcement and with bodies which are outside the self regulatory environment. These problems are discussed and some proposals are put forward as to how self regulation could be made more effective and provide a greater degree of assurance to the consumer of online information.

1. Introduction

On September 13, 2004, *Internet Law News* reported that the US financial intermediary PayPal was going to levy a 'fine' of up to $500 on customers who violate its use policies – i.e. on those customers who use PayPal to pay for gaming, pornography ('adult content') and pharmaceuticals from unregistered pharmacies [2]. The new policy, which took effect almost two weeks later and applies to both buyers and sellers, marked the first time PayPal imposed fines for violations of its use policy. Although *Internet Law News* speculates that PayPal had been pressed by regulators to take this kind of step, the company denied it.[2] Given this initiative, a highly interesting question would of course be: will the PayPal scenario become the politics of every intermediaries in these days of enforcement actions against anyone the regulators or any other interested party (e.g. copyright holders) can find? Whatever the answer to this question may be, the PayPal initiative is indeed a clear sign of the growing pressure on Internet intermediaries to introduce enforcement policies against bad and/or untrustworthy Internet content. And this in turn raises the interesting question of what exactly 'bad' or 'untrustworthy' Internet content is. Simple scenarios are, of course, related to content containing child pornography or clear violations of copyright. However, imagine a scenario where a consumer orders some medically necessary drug online and his financial intermediary docks his credit card for $500 because the pharmacy he ordered from happened not to have the right kind of license.

[1]This article was written as part of research project on the quality of health information on the Internet, subsidized by the Netherlands Organisation for Scientific Research (NWO).

[2]Given that PayPal was sued in the past for processing payments related to Internet gaming (charges laid under the Patriot Act), this initiative could have been a measure to forestall other actions.

In a world of information overload, it is often extremely difficult to get a grip on the correctness, completeness, and legitimacy of the information and material available on the Internet. Often a clear statement regarding the source of the information is lacking as well as the name, address and credentials of the information provider. Furthermore, providers fail to update their site on a regular basis and websites usually lack a statement describing what procedure and criteria were used for selection of the content. But even when these indicators are available, it still appears to be difficult for users (consumers, citizens or patients) to cope with the torrent of information on the Internet and distil out that which is most appropriate. When considering Internet content, clear differences arise between off- and online worlds. Litman [3] argues that: "*Some of this derived from the magic of digital technology. [. . .]. The ability to interact with the content you're reading changes your relationship with the content and that, eventually, changes both the way the content is written and displayed and what the content means.* In the offline world, distribution of information is structured through well-established channels. This allows for some form of 'filtering' of the information as well as focus on the specific audience for which it is intended. In contrast, the online world offers any individual the potential to distribute and consume any information that they wish. Health-related information is a good illustration of this. On the Internet, one can find professional medical or health-related information, commercial information on medical products and information based on individual experiences of patients as well as quacks. The characteristics of the online information chain are a clear example of the new opportunities that Internet offers to consumers in reinforcing their positions.[3] In the offline world, producers usually act as the first link in the information chain. Consumers are positioned at the end of the chain and can do nothing more than accept the information on products. In the online world, individual citizens and consumers can take the initiative and create the chain ('chain reversal'). 'Looking and (automatically) comparing' has become considerably easier on the Internet, especially when using (intelligent) search agents such as Google and MySimon. Dissatisfied patients or concerned lobbyists can use the Internet to make their dissatisfaction, interest or other feelings and ambitions known to a worldwide audience. Features such as self-organisation, self-help, self-publishing, worldwide distribution by pushing a single button and electronic social interaction appear to be key instruments in creating a whole new information environment. In other words, in addition to a rise in the quantity of information, the electronic environment also offers important new publication as well as medical services opportunities and thus whole new sources of information and service distribution.

This contribution does not aim to discuss criteria for evaluating the reliability or trustworthiness of content in an electronic world [8]. Instead, we focus on an issue that is related to the quality criteria debate. For in the realm of the debate on bad and untrustworthy Internet content and the search for reliability criteria, lies the question: what is, or could be the role of regulatory initiatives in addressing content that is bad and/or unreliable and, what is the legal status of the various efforts (guidelines, trustmarks and other quality schemes) that try to limit the risks involved in bad and unreliable content? Further on in this chapter, we want to make a contribution to the quality criteria debate from the legal perspective, and thus analyse the potential of instruments of self-regulation in addressing content-related risks in an online environment. In doing so, we will not deal with the obvious examples of 'bad' Internet content, such as child pornography and software or film piracy. Instead, we will focus on the more troublesome area of (un)reliable information. The key questions that we will be dealing with below are:

[3] Some of the key words describing this new position are 'consumer sovereignty', 'mass individualism' and 'demand-based supply' [5].

– What structures of self-regulatory control and private rulemaking could be used as instruments in enhancing the quality and trustworthiness of information? And
– What legal implications could arise when private initiatives regarding quality measures are taken?

Addressing the latter question appears to be of particular importance when looking at developments in the area of Internet Service Provider (ISP) liability. Court rulings in the US show that an ISP that explicitly markets itself as a provider which, as part of its value-added services, controls the distributed information and prevents the publication of inappropriate messages, can be held liable if he fails to do so.[4] The unfortunate result of these rulings is that an ISP – from a liability perspective – should do as little as possible to monitor and edit the content of the information it distributes. We will discuss the implications of this 'principle' in light of the development of measures to enhance the reliability of information, and propose an alternative way to deal with this issue. Finally, this article aims to provide some indications on what type of quality criteria and what enforcement mechanisms appear to be relevant when addressing unreliable information through regulatory measures. As will become clear, information is so flexible and diverse that it seems to resist attempts to regulate its quality. But first we will start of with a brief introduction to trust, online information and regulatory dimensions.

2. Trust, regulatory challenges and online information

Trust deals with belief, or the willingness to believe, that one can rely on the goodness, strength, and ability of somebody whether they are the seller or the buyer or in something, for example, certain online information. Of course, trust is highly subjective. It is the expectation that arises within a community where regular, honest, and cooperative behavior is the norm, and is based on commonly shared standards. Some of the trustworthiness that is a matter of fact in conventional communication of certain information no longer exists in electronic information delivery. For instance: an http address (URL) is not as reliable as a physical address; verification of an identity by means of a passport or a driver's license is not possible virtually; changes in a paper document are more easily detected than in a digital document; confidentiality of information is more easily guaranteed in a physical encounter (e.g. in a dialogue with a consultant or other professional) than in a virtual encounter. These securities, however, are of essential importance for the success of electronic information distribution and use. In addition to the trustworthiness of the information channel and the electronic communication itself, attention should be given to the trustworthiness of the information that is distributed and used, as well as the procedure followed.

Do we need new forms of trust in an electronic environment? How, otherwise, can parties know, whether certain information is of the required quality or whether the individual claiming to be a professional is indeed this person? Thus, the challenge lies in the perceived trustworthiness of the potential partners in the information chain. Of course, reputation, previous experience, and the size of the company that distributes the information may influence the perceived trustworthiness but the law may also play a role. For trust between parties can be enhanced by legislation (e.g. consumer protection), self-regulatory mechanisms (trustmarks, codes of conduct) and agreements (e.g. general terms and conditions, privacy agreements). A formalization of certain quality protocols could, for example, lead to more trustworthy ways of distributing and using information. On the technical side, trust in online information can also

[4] See: *Stratton Oakmont Inc v. Prodigy Services*, 1995 NY Misc., 23 *Media L. Rep.* 1794. Compare to *Cubby v. CompuServe*, 766 F. Supp 135 (SD NY 1991).

be enhanced by using technologies such as cryptographic applications; digital certificates to ensure both the authenticity of information and that of the persons behind this information; digital signatures and time-stamps to secure the authenticity of information and documents; encryption to protect information. However, these technological means for building trust do not always fit seamlessly into the legal system. Consequently, the legal system is currently finding a way to deal with the shifts in the basis of both instruments in online information and in trust. One of these areas is the legal status of self-regulatory instruments used to enhance trust in online information.

3. The challenge for self-regulatory mechanisms

A brief glance at the Internet shows that self-regulatory instruments[5] appear to have an increasingly substantial role with regard to the regulation of social and economic relationships. The rise of self-regulatory mechanisms is due to characteristics such as direct relationships between providers and users, simplicity, interactivity and flexibility. Moreover, the Internet transcends geographic frontiers. Thus, parties may wish to use codes of conduct and contracts to eliminate the differences between the various legal systems around the world. As a result, the cross-border dimension of Internet provides an excellent basis for experiments with private agreements between parties. Finally, the argument has been put forward that only the actors themselves are capable of perceiving the risks involved in particular types of electronic communication, business or use of services. Thus, the adoption of a code of conduct or some other self-regulatory instrument would assure a set of norms and sanctions tailored to the specifics of the situation.

The key challenge for all self-regulatory initiatives appears to be their enforcement. Although many responsible organisations try to ensure the adherence to the norms, either by sanctions and or by means of labelling and rating mechanisms, the characteristics of the online world make it difficult to effectively apply sanctions when parties fail to respect the set norms. Ensuring that the initiative passes from letter to action appears, in particular, to be difficult in light of the borderless environment in an online world. Furthermore, given that self-regulatory sources are often localized only in a certain territory, or that the initiatives are often limited to a group of actors that share a certain attitude towards professional behaviour, one may question the overall effect of self-regulatory initiatives. For if an organisation lacks the means, power and authority to enforce its norms, then their value remains symbolic instead of real. If a site owner is not a member of the regulatory scheme, the owner is, of course, under no obligation to abide by the rules set by the self-regulatory body. In principle, self-regulatory mechanisms do not establish law. Legal rules are binding to all citizens in a certain country; regulatory rules are not for the simple reason that self-regulatory mechanisms are not created by democratic means such as control by an elected parliament. Thus, a third party that is not a member of the self-regulatory scheme is not obliged to follow any suggestions that the body might make. In fact, the party may do nothing. This appears to be a rather disappointing outcome of the instrument of self-regulation. However, a self-regulatory instrument will have a positive effect on the quality of the information made available by those organisations that adhere to the self-regulatory instrument.

Self-regulatory schemes often work with a code of conduct, stating what is considered to be 'reliable' information under the code and what actions are expected of those adhering to the code to ensure that

[5]The phenomenon of self-regulation, sometimes called 'soft' law, refers to norms that are voluntarily developed, accepted and administered by members and authorities of a certain community.

only reliable information is placed on the Internet. Those providing the information to the public often state publicly that they adhere to the code by, for example, attaching the applicable seal of the trustmark to their website. Such a public commitment raises the expectations of the general public as well as of specific information consumers. Such expectations cannot be waived when a dispute arises about damage as a result of harmful or misleading information. Thus, commitment to a code prevents a debate on the applicable norms.[6] The fact that norms, definitions and responsibilities have been made clear, makes it generally easier to win a possible liability case. Let us therefore look at the relation between liability and self-regulatory mechanisms.

4. Liability for self-regulatory mechanisms

To a certain extent, the instigation of liability proceedings is a risky undertaking. Costs are definitely going to be incurred while it is uncertain whether either successful results can be booked or a conviction can be secured. It may also prove impossible to execute a conviction. Therefore the risk of failure seems to be reasonably high in the liability cases. Moreover, in Europe the issue of liability for unreliable mass information is virtually *terra incognita*, making it difficult to predict the outcome of a possible court proceeding. Things become even more complicated if the parties involved reside in different countries, which is not uncommon in conflicts arising on the Internet. Paradoxically, the (high) risk of failure for the instigator of proceedings does not necessarily mean that certifiers of information face little or no risks. Certifiers have to contend with the fact that their issued trustmarks are accessible in every country in the world. This makes it difficult – given differences in culture and levels of education – to predict how a trustmark and the information it relates to will be interpreted by those seeking the relevant information. Apart from the risks of misunderstanding or misinterpretation, there are cultural and legal differences in how to deal with damage as a result of unreliable information: the propensity to sue will inevitably vary from country to country as will the law of liability.

When looking at the instrument of liability in relation to unreliable information, it is clear that with the assumption of liability of mass information providers, such as publishers, concerning the provision of unreliable information to the general public the law is generally reticent. There is hardly any case law in Europe strictly regarding the liability for mass provision of unreliable information.[7] In literature, it is assumed that reticence with respect to such liability is necessary.[8] There is more case law in the US, but the courts are no less reticent.[9] One of the situations in which liability is more likely than elsewhere is where a (certification) provider attaches a seal or certification to a product, service or information, thereby (implicitly) representing that it has taken reasonable steps to make an independent examination of the product, service or information endorsed and that it found this satisfactory.[10] If this knowledge about liability law is applied to the provision of information on the Internet, it is clear that the certifier of

[6] Where we have hitherto simply talked about the provider of the information it must be noted that in case of a self-regulatory scheme many parties are involved in the provision of information: the provider of the information, the information-intermediary, a trustmark licensee, a custodian of a trustmark and a medical expert who reviews the information that is to be published.

[7] See e.g. BGH 7 Juli 1970 Neue Juristische Wochenschrift 1970, p. 1963 (Carter-Robbin-Test) and TGI Paris 28 Mai 1986 Revue trimestrielle de droit civil 1986 (3) juill.-sept., p. 552 (Fruits et plants comestibles). In the first mentioned case the editor was not found liable, in the second he was.

[8] Druey ([1, p. 135]) states: 'Die Freiheit der Information bringt mit sich, dass es grundsatzlich weder im öffentlichen Recht noch im Privatrecht einen allgemeinen Schutz gegen schlechte Information [. . .] gibt'.

[9] For an overview, see [7].

[10] See Hanberry v Hearst Corp. 81 Cal. Rptr. 519 (Cal. App. Dist. 1969).

certain types of information on the Internet is the link in the information distribution chain that is most exposed to liability risks.[11]

Liability for self-regulation, thus, may have a two-sided effect. On the one hand, it may spur the providers of information to take even greater care with the quality of the information. However, on the other hand, it may make information providers spurn self-regulatory schemes. They may fear that their efforts to enhance the reliability and quality of their information will turn against them. They fear that even a small mistake may be mercilessly exploited to bring a liability claim to a successful conclusion. Here, an interesting implication may arise from attempts to enhance the reliability of information because, following the reasoning of the Prodigy case decided in the United States, providers of reliability services that profile themselves as such, could be held liable for their added-value services. Prodigy was found liable for publishing illegal material.[12] The provider had explicitly marketed itself as an ISP (Internet Service Provider) and, as such, it would control and prevent the publication of inappropriate messages. Such an active approach led the Court to conclude that Prodigy was liable for not adequately checking the material it published. If this ruling is applied to reliability-conferring organisations, the Prodigy principle could imply that organisations taking an active role in checking and, where necessary removing Internet content, run the risk of being held liable, whereas those who do nothing avoid liability. The chilling-effect of the liability regime on measures to enhance the reliability and quality is however, neither a strange nor a new phenomenon. The effect is a well-known feature under liability law. Any organisation profiling itself as a trustworthy organisation that guards over the quality of its services raises a certain expectation with the public. Such an expectation may very well be enough to base liability upon.[13]

Nevertheless, there may be situations in which the chilling-effect is considered undesirable in light of certain interests or objectives. The US Congress (USC), for example, has recognized the negative side effect of the liability regime for ISPs and provided for protection for Good Samaritan blocking and screening of offensive material: 'No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.' (Art. 47 USC 230). Hence, in the US an Internet Service Provider is given legal leeway to screen and block offensive material: screening and blocking does not make an organisation a speaker or publisher. The question thus arises whether the interests in enhancing the quality of certain types of information, e.g. health-related information, may also justify an exemption under liability law. At first sight, one could argue that such interests indeed apply. The initiatives aim to enhance the quality of a highly 'sensitive' type of information, i.e. information that focuses on the health and well being of people. Unreliable health-related information may involve particular risks and there is a clear societal interest in stimulating measures to screen and block unreliable information. The above-described chilling-effect may have unwanted implications.

A closer look reveals that a liability exemption for certain types of information may have negative consequences. First, what should be done with providers of quality mechanisms (such as trustmarks) that fail to apply the expected level of care? Second, the afore-mentioned US approach has not been followed in other parts of the world. The European Union Directive on E-Commerce does not provide

[11] Apart from the implicit representation other factors have to be considered as well, e.g. whether the provider of the seal acted commercially or whether the seal constitutes an inducement to buy or use the product, service or information to which the seal is attached. Dependent on the case at hand, these factors may or may not make liability of a trustmark provider more likely.

[12] *Stratton Oakmont Inc v. Prodigy Services*, 1995 NY Misc., 23 *Media L. Rep.* 1794.

[13] Compare in this respect the liability of banks for unreliable prospectuses when issuing stock.

for such far-reaching protection.[14] In applying the European regime to trustmarks, we note that an organisation managing a trustmark scheme for reliable 'third party' information is not covered by the exemptions in the Directive since what the organisation does is more than merely transmitting or storing information. The organisation arranges for information to be evaluated, and allows a trustmark to be attached if the information complies with certain reliability criteria. If and under what conditions such an activity gives rise to liability is to be determined under the national laws of liability of the Member States of the European Union. Often, no clear-cut answer is available under the different national laws. As the US exemption approach under Article 47 USC 230 is not followed in other countries around the world, we are then confronted with the question as to which of the legal regimes applies, given that the online world is a world without borders. Are there other options available to address the unfortunate effect of liability for organisations that take an active role in Internet control? Are mechanisms available that mitigate liability without directly establishing immunity for liability? We think there are, and we would like to propose an alternative approach.

5. An alternative approach

The very essence of a trustmark scheme is that it presents itself as a trustworthy party; it claims implicitly or explicitly that users can depend on the information that is cleared by its scheme. As we concluded above, such a 'presentation' tends to enhance the standard by which the conduct of the trustmark manager scheme is measured. One could say that this standard tends to be measured by the end-result. If the cleared information appeared to be unreliable, the trustmark has failed to act according to expectations and is thus liable. To improve the liability position of trustmarks, we propose not to focus on the result, i.e. did the trustmark make sure that only reliable information was 'awarded' an authenticated graphic mark? Instead, we suggest determining liability on the basis of an established set of minimum measures to be taken by trustmark manager. Within this approach the liability standard will (with the understanding that not everything is foreseeable) concentrate on the specific implementation measures required to make the trustmark scheme reliable and less on the result.

Of course, this alternative approach would mean that careful consideration should be given to what exactly can and must be expected from trustmarks to ensure the reliability of information. For example, what requirements must the information meet? What measures must be taken to ensure that the information meets these requirements? What measures must be taken to ensure that the logo is not used without authorization? How can the persons providing the information be identified? Clearly, establishing such criteria (to be laid down in, for example, a code of conduct) is a challenge in itself. Also, the suggested approach has its downsides. The regime would be less flexible and it would hinder anonymous information distribution.[15] However, the benefits are clear. First, contrary to a liability exemption as established under the previously discussed US regime, the manager of a trustmark must

[14] As is apparent from recital 42: 'The exemptions from liability established in this Directive cover only cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient; this activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored.' Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, OJ L 178, 17 July 2000.

[15] See Nicoll and Prins [4] on the issue of anonymity.

take certain efforts to guarantee the reliability of information (i.e. make sure that the scheme conforms to rules of the code of conduct). Second, a trustmark manager who does not conform to the code can still be held liable for possible damages. Third, the person who suffers damages can always hold a person or organisation liable for these damages. Finally, the regime will give trustmarks managers some feeling of a safe harbor in establishing that they are exempt from liability if they acted according to the code of conduct.

In the meantime, how do private initiatives deal with possible liability situations resulting from trustmarks and other reliability enhancing mechanisms? A search through various websites that use reliability enhancing instruments reveals that many use disclaimers.[16] By using disclaimers they waive their liability. It may be no surprise that in the context of quality instruments, disclaimers appear to be a bit out of place. As mentioned earlier, there is in itself nothing wrong if an organisation implements certain measures to downplay the liability risks it may face. However, the organisations on which we have focussed in this particular case are those dealing in trust and enhancing quality. A disclaimer appears to be a bit of an odd instrument here. The consumer's trust in the quality of information will not be enhanced if those who provide the information or check its quality walk away from each and every liability. A brief glance at the terms and conditions of some of the organisations providing reliability instruments shows however that disclaimers are widely used. Two illustrative examples:

- "Although we carefully review our content, X cannot guarantee nor take responsibility for the medical accuracy of documents, we publish, nor can X assume any liability for the content of websites linked to our site."
- ". . . X et Y, ne sauraient etre rendues responsables de tout préjudice, direct ou indirect, de quelque nature que ce soit, résultant de l'utilisation, même partielle, des information de ce site".

It would reinforce consumer trust if the persons providing or checking the information would at least to some extent carry the burden if damages were suffered as a consequence of the consumer's reliance on this data. We believe that such an approach is not too far-fetched. Disclaimers are not all homogeneous. They exist in various forms and lengths and can thus be tailored to the needs within the specific context they are used. So, if for example, little money can be made from making information available on the Internet, a disclaimer could reflect this by maximising the amount of compensation payable to a user. If insurance coverage of the cost of liability is available, then the maximum cover and/or the maximum insurance compensation for damages payable could be stated. These and other aspects can be reflected in a disclaimer. If the efforts to heighten the quality of health-related information are to protect the health of individual persons, then a disclaimer could state that purely economic loss is not grounds for compensation. In other words, liability for information provided should be well considered. Neither denying the existence of liability, nor exaggerating it will lead to satisfactory results. Liability calls for an active approach, whereby the real issues are discerned, so that liability can fulfil a useful role in enforcement of self-regulatory schemes without 'overdoing it'.

6. In search of legally relevant quality criteria

In discussing enforcement scenarios for self-regulatory mechanisms one final interesting question arises. Do self-regulatory initiatives have an external effect, i.e. can a code of conduct adopted by

[16] It should be noted that disclaimers on websites may or may not, and under certain conditions, be valid in all jurisdictions.

representatives of certain actors, influence or even determine the required behaviour of actors who are not a party to the code of conduct? Although the recognition of such an effect would not guarantee an optimal sanctioning and enforcement of violations of the private norms, it may certainly contribute to the efficacy of such norms. A step further is a situation in which the adopted norms, such as quality standards for information, may become a professional standard whereby contravention automatically constitutes a fault. This would create a situation in which self-regulation becomes a key source of law complementary to the rules issued by the government, and could perhaps even replace the latter. Is it realistic in that the quality criteria for electronic information become more than just the professional standard, but also a *de jure* standard? An answer to this question requires a discussion on the legal status of self-regulatory initiatives versus third parties.

We already mentioned in the previous section that self-regulatory mechanisms do not establish law in the meaning of legal rules that are binding to all citizens in a certain country for the reason that the self-regulatory mechanisms were not created, discussed and adopted by democratic means such as control by an elected parliament. In addition, scholars of private law have been either reluctant to debate the status of self-regulatory mechanisms under private law or even completely ignored such a discussion. Given, the prominent role expected of self-regulatory mechanisms, at least in an online environment, it appears high time that such a debate is put on the agenda.

But even if self-regulatory mechanisms were to gain importance under private law, many other important questions arise. What criteria should decide upon the 'quality' of certain types of information? What about the status of possible contesting criteria? Who will be responsible for drawing up the criteria and what about meaningful participation of all those affected by the adopted criteria? All of these questions bring us to the legitimacy of the process and the criteria needed to define when a self-regulatory mechanism can claim legitimacy. Below, we will try to distil legal duties from reliability criteria and thus make a contribution to the scientific discussion, from a legal perspective, on 'categorizing' quality criteria. We thus intend to explore, what could be gained by establishing 'new' rules to deal with the reliability of information and, what difficulties have to be overcome. This will be followed by a tentative sketch of such an approach.

Approaching the regulatory dimension of the reliability of information from a liability perspective – which is the traditional approach – introduces a certain bias in the duties that rest upon those who provide and (ought to) check information. The duties focus on avoiding anything that could be a link in the causal chain leading up to damage though reliance on the information. A typical example is a duty stating that information must be accurate. Inaccurate information can lead to damage, if somebody relies on it. A new approach to regulation would be to try to distil duties from criteria for reliability. To a certain extent this leads to other duties. One of these duties could be, for example, the duty to mention the name and quality, e.g. profession, of the author or a certain type of information, e.g. medical or financial. From the traditional liability perspective, not mentioning a name or quality could hardly be relevant because the omission of such information could seldom be the cause of the damage somebody suffered because they relied on the information given. However, when one considers the perspective of reliability duties, mentioning a name and quality appear to be very important. Put differently, where the focus of liability law and ensuing duties is on avoidance and causation of damage, the focus of reliability criteria and ensuing duties is more on user empowerment and making the reliability of information verifiable.

If the reliability duty approach were to be taken, use of the liability law regime would only be useful to a limited extent; the new approach would require the development of criteria and rules that may hardly be relevant in the context of liability. These rules would need to be established outside and independent of the regime of liability law. The 'diverging' rules could be formulated as a code in the context of a

self-regulatory initiative or as statutory law. The former may, for the time being, be preferable. The development of new rules will have to gain acceptance and, self-regulation can act as basis to build up such rules. Competing self-regulatory schemes may exhibit different rules and thus create a pool of rules from which to choose. By fostering the online presence of established credibility-conferring institutions, indications will appear on what criteria and rules function best. In the long run, such rules could (perhaps) be upgraded to *de jure* norms.

The course proposed here should however not be thought of lightly. Translation of reliability criteria into duties is far from a straightforward job. To illustrate the challenges, we shall sketch just a few of the 'problem areas':

- Experts generally know in how much detail they have to explain certain issues to their colleagues. However, when certain specialized information is available freely on the Internet it is also used by non-experts. What should then be the scope of the ensuing 'duties' in providing and checking the information? Should these important duties be ignored if they state that the information is only for experts?
- Consistency, coherence and accuracy appear to be important criteria, just like interpretability and accessibility. For an author, this implies that he or she has to make the information consistent, coherent, accurate etc. However, when trying to translate these criteria into legal norms, one comes across the problem that these qualities are difficult to measure. In general, legal norms should be sufficiently clear so that those, to whom the duties are directed, clearly understand what is expected of them. How can these duties be enforced? For example, what level of inconsistency is sufficient to take enforcement measures (in the absence of damage)?
- Information should conform with observations and consensus. The user of information can be helped by references to such observations or consensus. But, forcing an author of information to refer to sources puts a burden on their shoulders because it is not clear exactly how much research into observations and consensus is required.
- Finally, key criteria to determine reliability are authority, trustworthiness and credibility of the persons or organisations behind the information. These criteria may, perhaps, be translated into a duty to identify the persons and organisations behind the information. It is however, not clear how this relates to the 'good' intentions an individual may have to want to remain anonymous or act under pseudonym? Do we follow the approach taken under the European Union e-Commerce Directive and require that providers of information society services provide certain information (among which information on their identity)? How would this relate to citizens, consumers or patients who wish to communicate about their situation or condition in an anonymous way?

7. Conclusion

The distribution and presence of unreliable information on the Internet appears to be a problem of growing importance. Clearly, risks arise as a result of this information. Considering the possible negative consequences, it appears desirable that the law plays its part in addressing this problem. Traditionally, the law approaches the unreliability of information as a liability problem. This approach appears however to be insufficient [6]. As has happened in many other areas where a new normative solution to 'online' problems have been sought, self-regulatory mechanisms appear to be an interesting option. In many areas of online regulation, self-regulation has proven to provide a sound basis to develop new rules. Based on the earlier experiences, we have discussed possible new rules that may help enhance the reliability

of information on the Internet. These rules need to address those that provide and check information and guide them towards more reliable information. Besides the organisational measures such as user education and by making the reliability of information more transparent and thus verifiable, a regulatory approach enhancing reliability seems to be the establishment of criteria for the quality of information. Based on this view, we have proposed a different approach to regulating the reliability of information in an online environment. The discussion also showed that the step from reliability criteria to enforceable norms that regulate the behavior of the providers of information appears far from trivial. The very characteristic of information is that it is so flexible and diverse that it seems to resist every attempt to regulate it. Nevertheless, we feel that in addressing the reliability of information on the Internet one must look beyond the borders of the traditional regulatory mechanisms (e.g. liability law) and look for possible new approaches. We hope in this contribution to have made some tentative steps towards another approach.

References

[1] J.N. Druey, *Information als Gegenstand des Rechts, Entwurf einer Grundlegung*, Zurich: Schulthess Polygraphischer Verlag, 1995.
[2] Internet Law News, *PayPal to levy fines for gambling, porn*, available at: http://news.com.com/2100-1026_3-5362576.html, 2004.
[3] J. Litman, Electronic Commerce and Free Speech, in: *The Commodification of Information*, N. Elkin-Koren and N. Weinstock Netanel, eds, The Hague, London, New York: Kluwer Law International, 2002, p. 26.
[4] C. Nicoll and J.E.J. Prins, Anonymity: Challenges for Politics and Law, in: *Digital Anonymity and the Law. Tensions and Dimensions*, C. Nicoll, J.E.J. Prins and M. van Dellen, eds, The Hague: T.M.C. Asser Press, 2003, pp. 287–297.
[5] J.E.J. Prins, Consumers, Liability, and the Online World, *Information & Communications Technology Law* **12**(2) (2003), 143–164.
[6] J.E.J. Prins and M.H.M. Schellekens, The Chilling-Effect of Liability Law on Initiatives to Enhance the Reliability of On-Line Health-Related Information, *European Journal of Health Law* **11** (2004), 201–207.
[7] J. Rothstein Wolfson, Electronic mass information providers and section 552 of the restatement (second) of torts: the first amendment casts a long shadow, *Rutgers Law Journal*, **29**(1) (2001).
[8] A. Vedder and R. Wachbroit, Reliability of Information: Some Distinctions, *Ethics & Information Technology* **6**(1) (2004).